

REMARKS

Claims 29, 31, 32, 35, 36 and 38-43, as amended, remain herein. Claims 41-43 are new. Claims 33 and 37 are canceled without prejudice. Claim 41 replaces former claim 33. Claims 35, 36, 39, 40 and 42 are dependent upon independent claim 41. Claims 31, 32, 38 and 43 are dependent upon independent claim 29.

1. Applicants and their undersigned attorney appreciate the courtesies extended by Examiners Fischer and West during the interview conducted at the PTO on July 20, 2010. While applicants presented to the Examiners, via facsimile before the interview, some draft arguments distinguishing applicants' claimed invention from the cited prior art, at the interview Examiner Fischer did most of the talking and focused on applicants' independent claim 33, rather than claim 29 or the prior art. Examiner Fischer suggested that several elements of claim 33 were inferentially recited, rather than affirmatively recited as elements or limitations of the claimed method. Applicants have amended claim 33 to more affirmatively recite more elements or limitations of claim 33.

After his comments about the claims, Examiner Fischer concluded the interview without discussion of the cited prior art. Examiner Fischer did say that an Amendment responsive to the final Office Action of April 27, 2010 would be entered.

2. Claims 29, 31-33 and 35-40 were rejected under §103(a) over O'Boyle, Tanabe, Arii, and Waters.

The Method Claims

Applicants method claims 41, 35, 36, 39, 40 and 42 recite a method for reproducing data from an optical disk. Applicants' independent claim 41 recites steps for (1) reading a cipher key and identification information unique to an optical disk having data stored thereon, the identification information and cipher key having been recorded in the form of stripe patterns extending along radii of the optical disk by laser trimming a reflective layer of the disk; (2) encoding specific data by using the cipher key; and (3) the

. . . content reproducing device communicating at least the identification information and the encoded specific data to a server having therein at least one decode key that corresponds to the identification information from the disk; said server selecting a decode key that corresponds to said identification information from said optical disk, and decoding the encoded specific data using the selected decode key.

Applicants' claimed invention is schematically illustrated in the attached Exhibit 1.

Applicants' invention is advantageous in that two different elements, namely the identification information and cipher key, are recorded in the stripe patterns of the optical disk, and the cipher key is used to encode the data to be communicated to the server, and the identification information is transmitted to the server and used to select the decode key on the server. These elements make such communications safer by using the cipher key, and provide much higher security because any unauthorized optical disk having either invalid identification information or an invalid cipher key will be rejected by the selected decode key corresponding

thereto. In other words, both the identification information and cipher key must be valid to permit decoding of the encoded data.

In addition, by storing the identification information and cipher key in the stripe patterns, which are difficult to counterfeit, the security level is further improved.

Wholly apart from the improvement in security, because the decode key corresponding to the identification information of the optical disk is stored on the server, decoding the encoded specific data is facilitated because it can be done if the optical disk is valid.

If, for example, only the cipher key exists in a disk, with no identification information, whether the encoded specific data should be decoded is determined on the server which is the destination of the data, so it is necessary to pre-store the same information as the encoded data on the server to be able to compare the two pieces of information to determine whether or not the encoded specific data is identical to that stored on the server. This makes it necessary to encode in advance all of the data possibly received, and store all of that encoded data on the server.

In contrast, applicants' invention stores decode keys corresponding to the identification information of the optical disk, so applicants' invention can decode the encoded specific data simply if the optical disk is valid without storing all of the encoded data on the server.

The Device Claims

Applicants' device claims 29, 31, 32, 38 and 43 recite elements comprising means for (1) reading a cipher key and identification information unique to an optical disk having data stored thereon, the identification information and cipher key having been recorded by laser trimming a

reflective layer of the disk in the form of stripe patterns extending along radii of the optical disk;

(2) encoding data by using the cipher key; and (3)

. . . communicating certain information including identification information and the encoded specific data to a server capable of selecting a decode key that corresponds to the identification information and with the selected decode key decoding the encoded specific data.

See, again, attached Exhibit 1.

Each of the claimed reading means, encoding means, and communicating means is supported by applicants' disclosure. See, for example, FIGS. 6A and 6B, annotated copies of which are attached hereto as Exhibit 6A/B.

As illustrated in Figs. 6A/6B, in first computer 909 there is BCA reproducing part 820, which is the "reading means." In first computer 909, second cipher encoder 831 encodes accounting data 830, and thus is the "encoding means." In first computer 909, communication part 822 is the "communicating means." In addition, there is a second cipher decoder 832 that decodes enciphered accounting information in the third computer 828, which corresponds to a "server" in applicants' claim 29.

In applicants' specification, page 8, lines 28-32, there is disclosure of the structure of the reading means. At page 10, lines 29-335, there is disclosure of the structure of the encoding means. At page 11, lines 1-10, there is disclosure of the structure of the communicating means. See pages 8-11 of applicants' specification, copies of which are attached hereto as Exhibit 3.

The Cited Prior Art

O'Boyle '329 does not disclose or suggest applicants' claimed invention. O'Boyle '329 seeks to improve the security level of optical verification for holographic products or a combination of holographic and magnetic products in the form of a card or a security document. See the attached Exhibit 2 which schematically outlines the O'Boyle disclosure. Based on an account access identification number, an optical clock stripe 35 is formed in accordance with a hologram recording formed on the card. Through the counting operation using the optical clock stripe 35, a hologram-recorded Image Signal can be digitized into coded binary data so that Accountable Data is obtained. See O'Boyle '329, Figs. 6, 9, 11a, and column 9, lines 24-45.

According to O'Boyle '329, whether a card or security document is valid is determined as follows:

First, Accountable Data encrypted using encryption algorithm 25 is stored in advance in a given storage space (for example, computer, host, or hologram). When the data read from the card or security document, and similarly recorded using the optical clock stripe 35, are both consistent with the encrypted Accountable Data, the card or security document is confirmed as valid. See O'Boyle '329, Figs. 8, 10, 11b, and column 9, line 46 through column 10, line 54.

The Office Action admits that O'Boyle '329 fails to disclose any "stripe pattern extending in the radial direction." And, there are other technical elements of applicants' claims which are not disclosed in O'Boyle '329.

O'Boyle '329 does not disclose that between identification information and a cipher key, which are recorded in the stripe patterns of an optical disk, one of them, a cipher key, is used to

encode data to be communicated to a server, and the other, the identification information, is transmitted to a server and used to select a decode key on the server.

According to O'Boyle '329, a cipher key used to encrypt encoded Accountable Data is not recorded in the card, whereas applicants' claimed cipher key is recorded in the optical disk in applicants' claimed invention.

Further, O'Boyle '329 requires that the validity of the card be determined by directly comparing (i) encoded data read from the card, and (ii) the data previously encoded and stored. Therefore, the O'Boyle '329 system is different from applicants' invention wherein one of the elements, namely identification information, is transmitted to the server and used to select the decode key on the server. In applicants' invention, the disk containing the data is determined to be valid when both the identification information and cipher key are valid after selecting a decode key based on identification information on the server.

Thus neither O'Boyle '329 alone, or when combined with any of the other cited references, could achieve preventing decoding of encoded data from any unauthorized optical disk, even having either one of the valid identification information or cipher key. Further, neither O'Boyle alone or in combination with any of the other cited references would have suggested that it is unnecessary to encode all the data possibly communicated and store all of that encoded data in advance on the server.

Tanabe '767 does not disclose the stripe patterns of applicants' claimed invention. The stripe patterns of Tanabe '767 are made by etching, which is not unique to each disk and is easy to counterfeit. In contrast, the stripe patterns of applicants' invention are made by laser trimming

a reflective layer in each disk, which results in a unique stripe pattern for each disk. Applicants' laser trimmed stripe patterns are therefore very difficult to counterfeit. And, the identification information and cipher key are recorded in such stripe patterns, and the encryption of specific data using such identification information achieves a higher security level.

Similarly, Aarii '776 and Waters '589 do not disclose or suggest applicants' claimed laser trimmed stripe patterns.

Thus, each of Tanabe '767, Aarii '776, and Waters '589 fails to provide the deficiencies of O'Boyle '329.

There is no disclosure or teaching in any of O'Boyle, Tanabe, Aarii, and Waters, of all elements of applicants' claimed invention. Nor is there any disclosure or teaching in any of those references or anything else in this record that would have suggested modifying or combining same effectively to anticipate or suggest applicants' presently claimed invention. Thus, there is no disclosure or teaching in any of the cited references that would have suggested applicants' claimed invention to one of ordinary skill in this art. Reconsideration and withdrawal of the rejection are respectfully requested.

3. During the July 20, 2010 interview, Examiner Fischer said that the present application (S.N. 10/809,498) is not assigned, and questioned whether it is commonly owned with other Oshima et al. patents such as U.S. Patents 5,761,301 and 6,052,465. However, the present application and those two patents are all commonly owned by Matsushita (now named Panasonic Corporation). See Exhibit 4 attached. Applicants believe that neither of those patents

is effective prior art under either §102(e) or §103(a) as evidenced by the facts that (1) Messrs. Oshima and Goto are common inventors to those patents as well as the present application, and (2) neither of those patents discloses copy protection or encryption using BCA stripe patterns as in the present application.

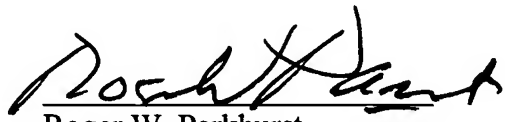
* * * * *

For all the foregoing reasons, all claims 29, 31, 32, 35, 36 and 38-43 are now proper in form and patentably distinguished over all grounds of rejection stated in the Office Action. Accordingly, allowance of all claims and a notice to that effect are respectfully requested. The PTO is hereby authorized to charge/credit any fee deficiencies or overpayments to Deposit Account No. 19-4293. If further amendments would place this application in even better condition for issue, the Examiner is invited to call applicants' undersigned attorney at the number listed below.

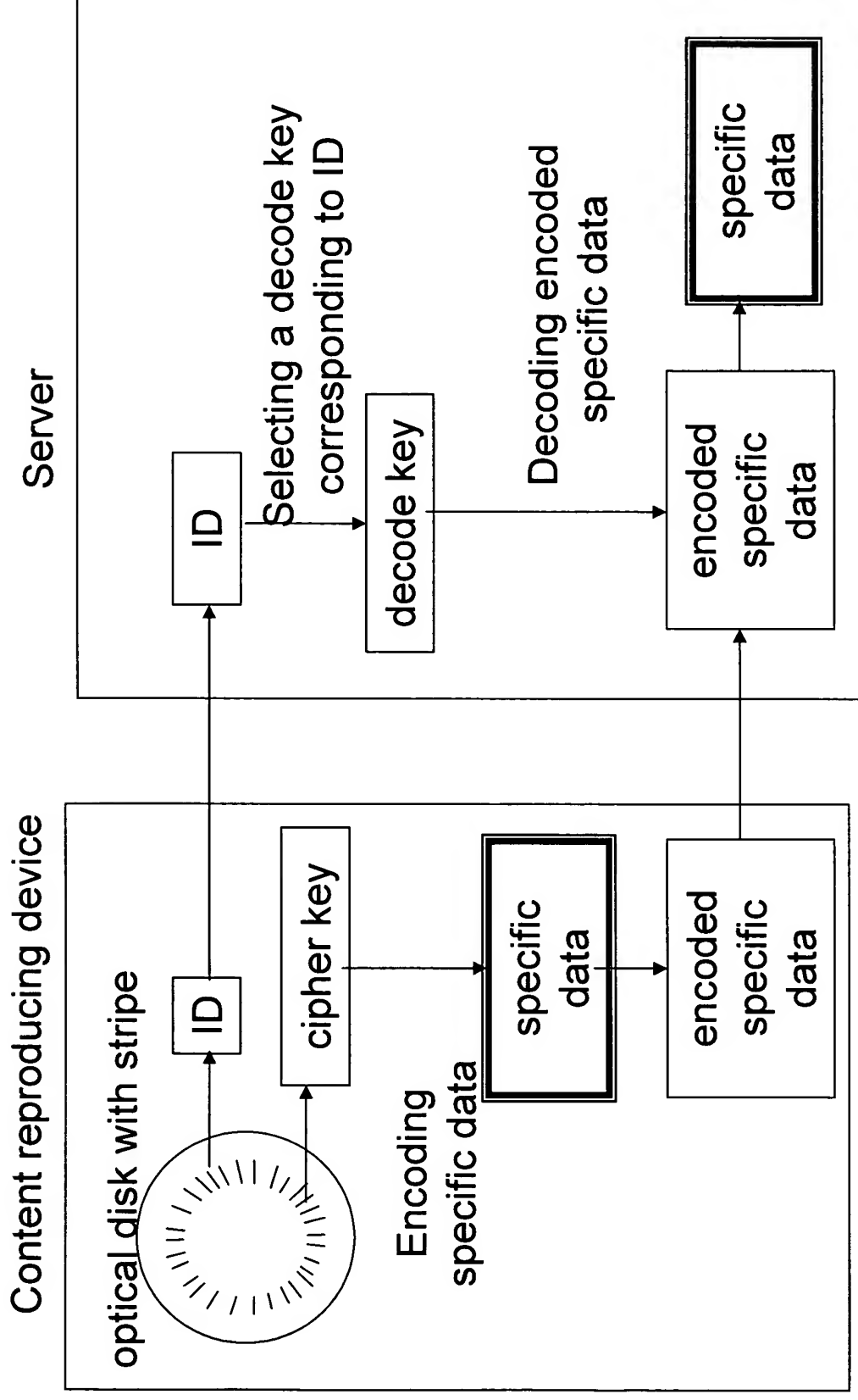
Date: August 23, 2010

STEPTOE & JOHNSON LLP
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036-1795
Tel: (202) 429-3000
Fax: (202) 429-3902

Respectfully submitted,


Roger W. Parkhurst
Reg. No. 25,177

Attachments: Exhibits 1,2, 3, 4 and 6A/B



Both ID and cipher key must be valid to properly decode encoded specific data.

EXHIBIT 1

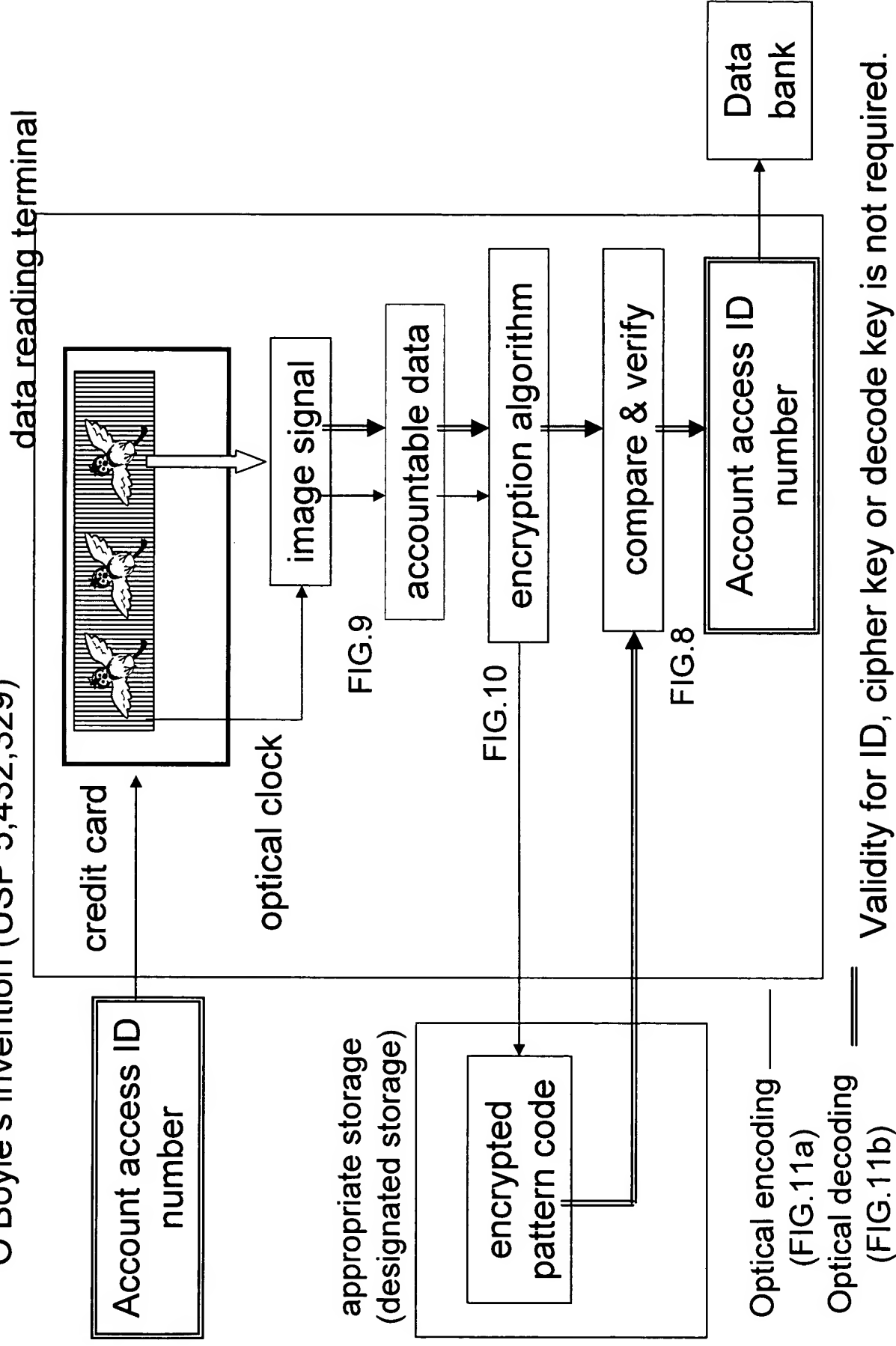


EXHIBIT 2

FIG. 6A

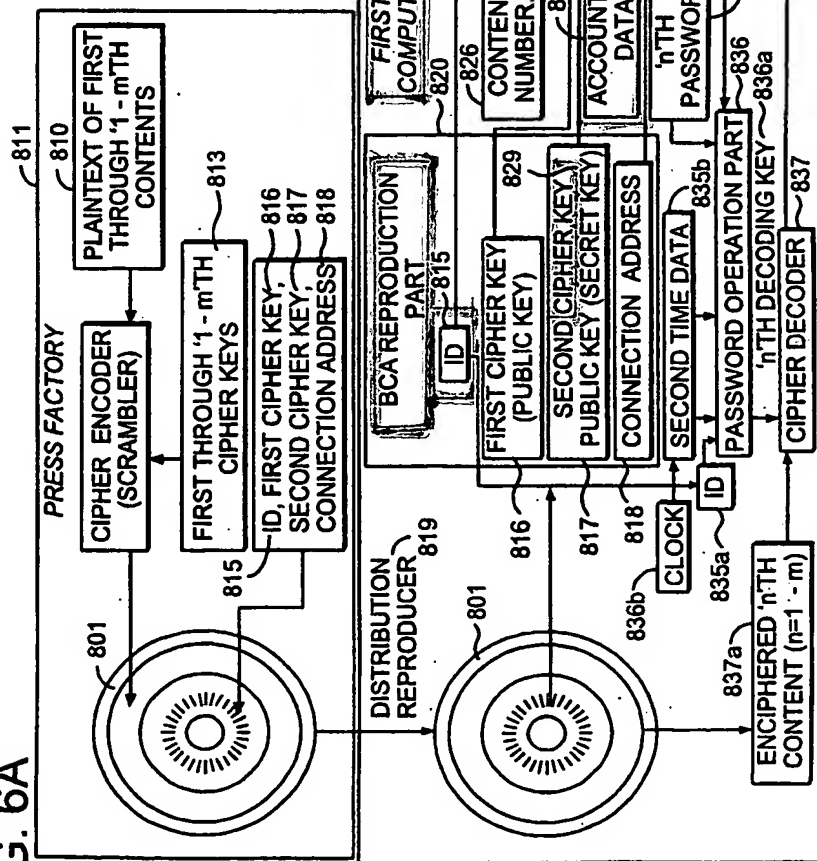
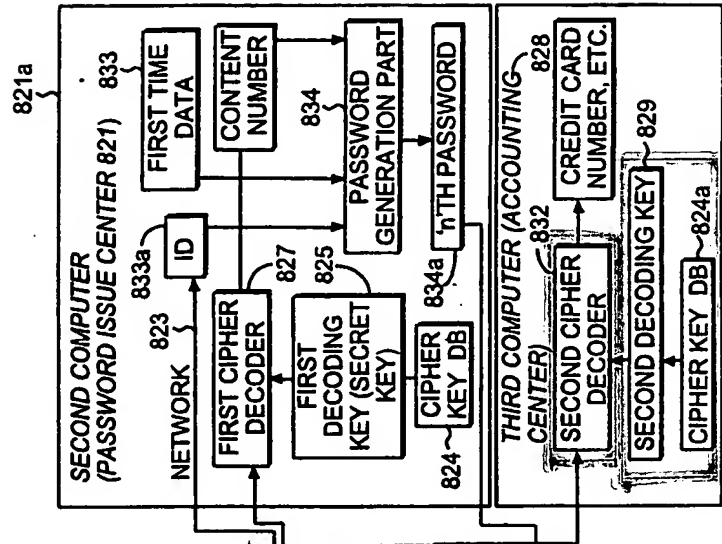


FIG. 6B



With reference to Fig. 6, the overall system of a cipher software unlatching system, narrowed down to the operations of password issue, cryptocommunication, and orderer certification, will be described. The steps in a press factory are nearly the same as in Fig. 1, so the original disk 800 and the completed disk 809 are not shown.

In a press factory 811, a cipher encoder 812 enciphers the data in the plaintexts 810 of the first to the '1- m'th contents or scrambles the picture signals therein with the first to '1- m'th cipher keys 813, respectively. The data or the signals are then recorded on an original optical disk 800. Disk-like substrates 809 are pressed from the original disk 800. After a reflecting film is formed on each substrate 809, the two disk-like substrates are laminated together. Thereafter a completed disk 809 is made. Recorded in the BCA areas 814 of completed disks 809 are different IDs 815 and/or first cipher keys 816 (public keys) and/or second cipher keys 817 (public keys) and second computer connection addresses 818 so as to make disks 801 each with a BCA. The disks 801 are distributed to users.

The contents of these disks have been enciphered. Therefore, in order to reproduce the contents of each of the disks, it is necessary to get a password from a password issue center, an electronic shop or a mall, by paying a charge. That procedure will be described next.

In a user's first computer 909, if a reproducer 819 reproduces a distributed disk 801 with a BCA, a BCA reproduction part 820 including a PE-RZ demodulation part reproduces the data of the ID 815, first cipher key 816, second cipher key 817 and/or connection address 818. In order to get a password, the connection address 818 of the second computer 821a, which is the server of a password issue center 821, is accessed through a

communication part 822 via the Internet or another network 823, and the ID is transmitted to the second computer 821a.

5 Here, the cryptocommunication procedure will be described. The second computer 821a receives the ID 815 from the user's reproducer 819. Then, the second computer or server 821a of the password issue center 821, which is called a 'mall' or an 'electronic shop' has a cipher key database 824. This database contains a table
10 of the secret keys which are the decoding keys corresponding to the disks' own IDs or the first cipher keys 816 of the IDs, that is the first decoding keys 825 and the IDs. The server can therefore search for the first decoding key 825 based on the received ID. Thus
15 cryptocommunication is completed from the first computer to the second computer 821a. In this case, if the first cipher key and first decoding key are common keys of a common key cipher, not of an public key cipher, they are the same key.

20 If the user wants to use part of the enciphered contents stored on the disk 801, which may be 1,000 in number, for example, the content number 826 of which is 'n', the user sends to the second computer 821a the cipher which is the content number 826, that is, 'n'
25 enciphered with the public key which is the first cipher key 816 by the first cipher encoder 827 composed of public key cipher functions. The second computer 821a searches for the first decoding key 825 for decoding this cipher as stated above. It is therefore possible
30 securely to convert this cipher into plaintext. Thus, the cipher protects the privacy of the user's order data.

In this case, a signature may be made by means of the secret key of the public key cipher as the first cipher key 816. This method is called 'digital
35 signature'. For a detailed explanation of the operation

of 'digital signature', see, for example, 'Digital Signature of E-Mail Security by Bruce Schneider 1995'.

Back to the cryptocommunication, the cipher is sent through the communication part 822 and network 823 to the
5 first cipher decoder 827 of the password issue center 821. Thus the first cipher decoder 827 decodes the cipher by means of the first pair cipher key 825 pairing with the first cipher key 816.

In this case, because only the one disk has the
10 public key, it is possible to reject invalid orders from third parties' disks. In other words, because each disk can be certified, it is possible to certify the user who owns the disk. It is thus certified that the content number 'n' represents a particular individual's order.
15 It is therefore possible to exclude invalid orders of third parties.

If the public key 816 is secret, this method can technically be used to send a credit card number, or other accounting data which requires high security.
20 Generally shops called 'malls' however, do not settle users' accounting data electronically, because there is no guarantee of security. Only the accounting centers 828 of credit card companies, banks and the like can deal with users' financial data. Presently, security
25 standards such as secure electronic transaction (SET) are being unified, so it is probable that Rivest, Shamir and Adleman (RSA) 1024 bit public key ciphers will be used and the encipherment of financial data will be possible.

Next, ~~the accounting data cryptocommunication~~
30 ~~procedure of the present invention will be shown.~~ First, by using the second cipher key 817 of the public key cipher reproduced by the BCA reproduction part 820, the
~~second cipher encoder 831 enciphers the accounting data~~
~~830 such as an individual's credit card number with a~~
35 ~~public key system cipher such as RSA.~~ The enciphered

encode

data is sent from the communication part 822 through the second computer 821 to the cipher decoder 832 of the third computer 828. In this case, if there is a need for digital signature, the secret key 829 is used as the second cipher key 817.

Similar to the procedure for the cipher key of the second computer 821a of the password issue center 821, it is possible to search the cipher key database 824a for the second decoding key 829 corresponding to the ID or the second cipher key 817. By using this decoding key 829, the second cipher decoder 832 can decode the enciphered accounting data.

If a digital signature is made by the second cipher encoder 831 with the secret key 829, the user's signature can be confirmed in the second cipher decoder 832. The accounting center 828 can thus get the user's credit card number, bank card number, bank password, or other accounting data safely even via the Internet. In open networks such as the Internet, security comes into question. By means of this system, however, it is possible to make cryptocommunication or certification without fault, because the cipher key (public key) for cryptocommunication or the secret key for digital signature has been recorded in the BCA. It is therefore possible to prevent third parties' unauthorized accounting and orders. In addition, because it is possible to use various public keys for different disks, that is, different users, the confidentiality of communication is improved, and the possibility of users' accounting data leaking to third parties is reduced.

Referring back to Fig. 6, the procedure for issuing a password and the procedure for unlatching with a password will be explained. The password issue center 821 includes a password generation part 834 with an operation expression of public key ciphers etc. Part 834

decode

10/809,498Recording medium, recorder, reproducer, cryptocommunication system
and program license system08-05-
2010::12:18:44**Parent Continuity Data**

Description	Parent Number	Parent Filing or 371(c) Date	Parent Status	Patent Number
This application is a Continuation of	10/418,088	04-18-2003	Patented	7,127,430
is a continuation of	09/475,228	12-30-1999	Patented	6,611,820
is a continuation of	08/849,468	06-09-1997	Patented	6,081,785
is National Stage Entry of	PCT/JP96/02924	10-08-1996	Published	-

Child Continuity Data**No Child Continuity Data Found**Close Window**EXHIBIT 4**